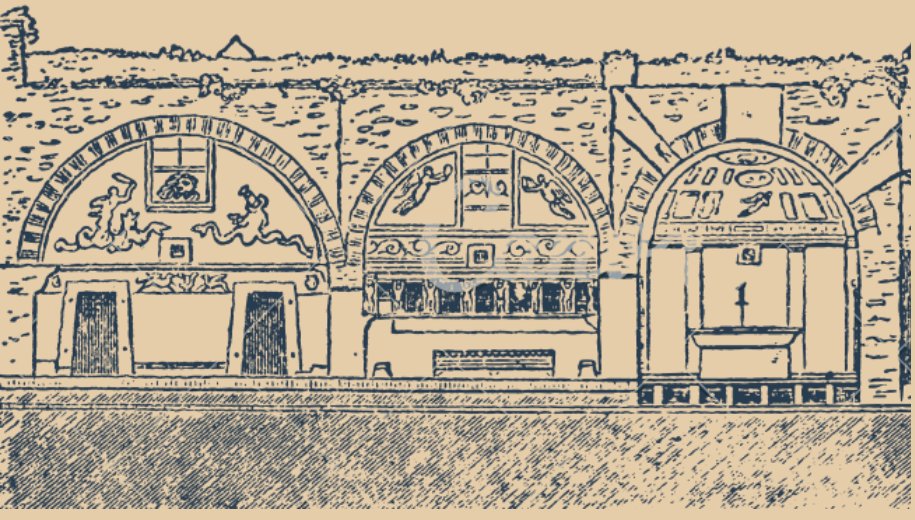
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 31 MAY – 06 JUNE 2026



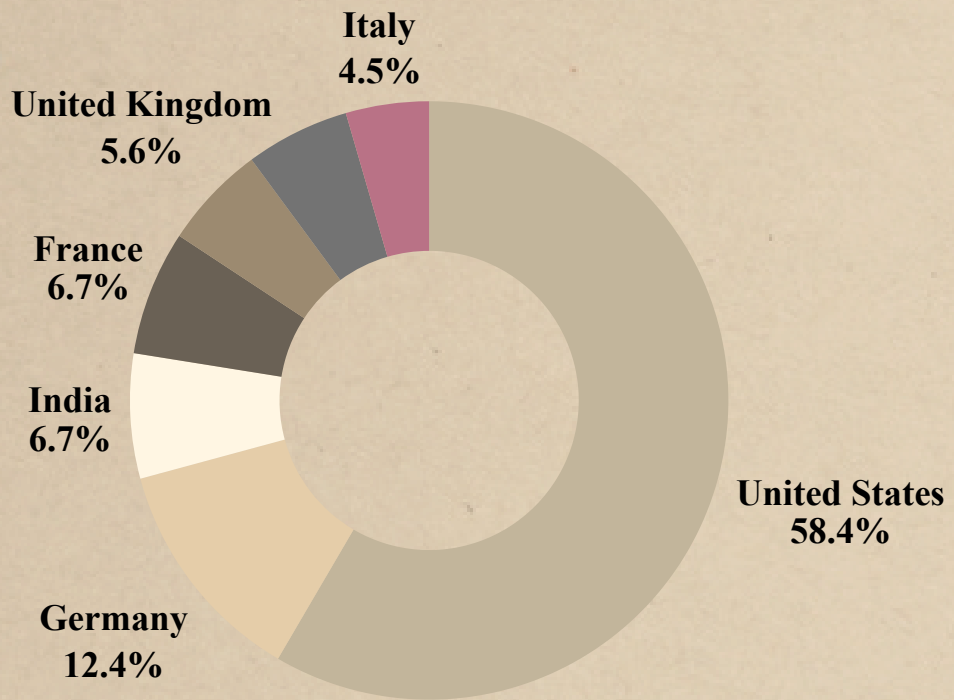
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:31 MAY - 06JUNE 2026

Overview

This weekly report provides an overview of global data breach activity linked to threat groups. It focuses on exposure patterns, threat actor activity, and key trends observed across industries and geographies.

Geographic Distribution



Key Highlights

- The majority of incidents were tied to ransomware and data extortion activity, reflecting the persistent threat posed by financially motivated cybercriminals.
- Threat groups such as **The Gentlemen**, **InCransom**, **Qilin**, and **Akira** were repeatedly observed, indicating ongoing and coordinated attack campaigns.

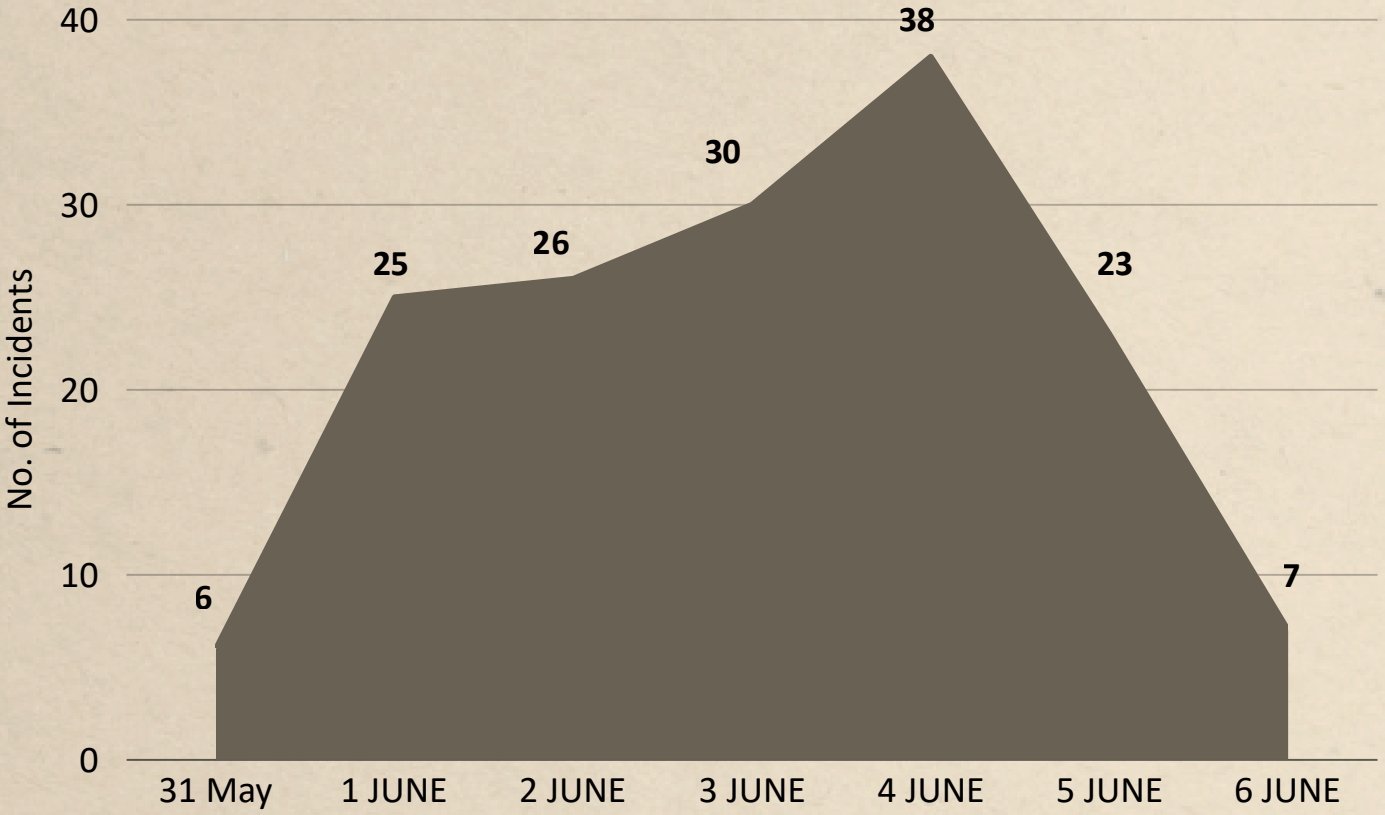
Most Targeted Sector: Manufacturing
Ransomware-linked breaches: 81.9%

Total Breaches Observed: 155
Countries Affected: 44

GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:31MAY - 06 JUNE 2026

Breach Over time

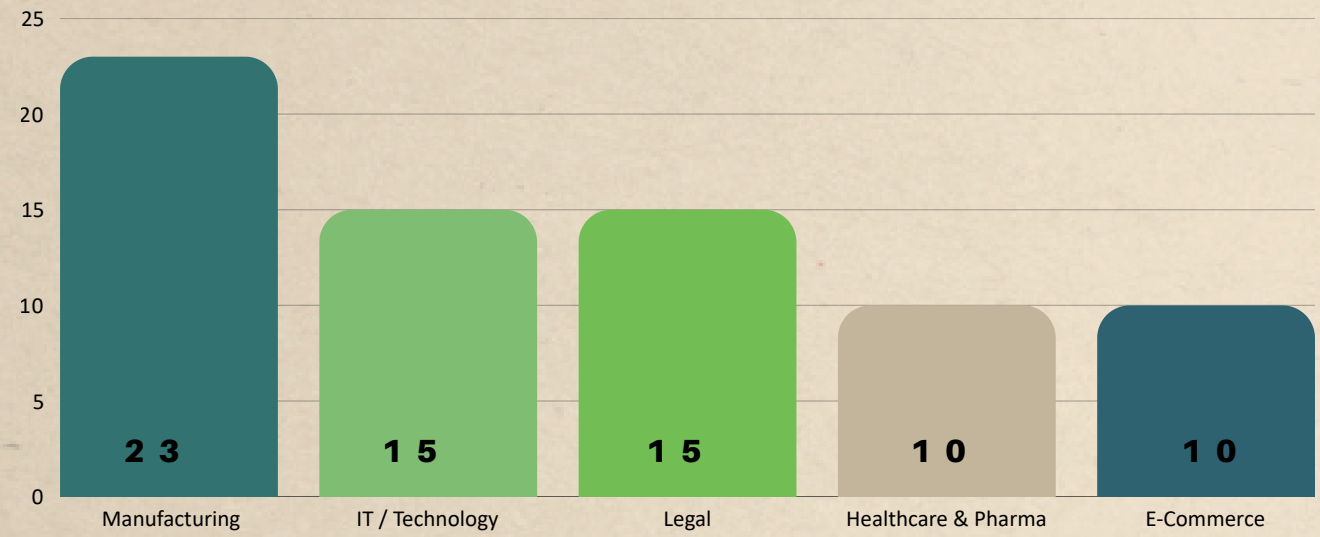


- Breach activity fluctuated throughout the period, with June 04, recording the highest spike at 38 reported incidents.
- A sharp rise was observed between June 2 and June 3, peaking at 30 incidents on June 3, indicating intensified disclosure or attack activity.
- May 31 reported the lowest number of incidents, with only 6 breaches observed.
- Overall, the trend reflects irregular but high-impact surges, followed by short periods of decline and stabilization.

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:31 MAY - 06 JUNE 2026

Affected Sectors



Industry Highlights

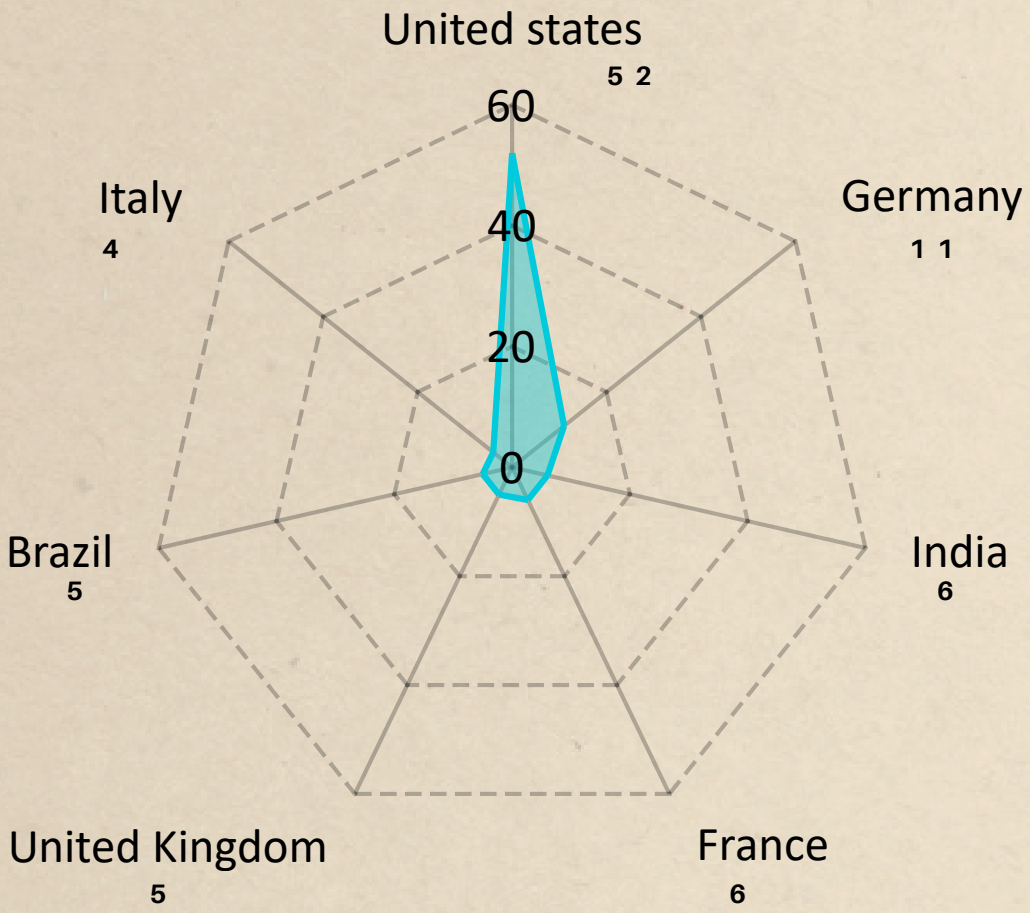
- **Manufacturing & Engineering: 23+ incidents (highest targeted sector)**
- **IT / Technology: 15+ incidents (high exposure due to digital infrastructure)**
- **Finance / Legal / Insurance: 15+ incidents**
- **Healthcare & Pharma: 10+ incidents**
- **E-Commerce : 10+ incidents**

Industries Insight: Manufacturing remained the most targeted sector, while technology and financial organizations saw sustained activity. Healthcare and retail sectors also experienced notable targeting, reflecting attackers' continued interest in organizations handling sensitive data and critical operations.

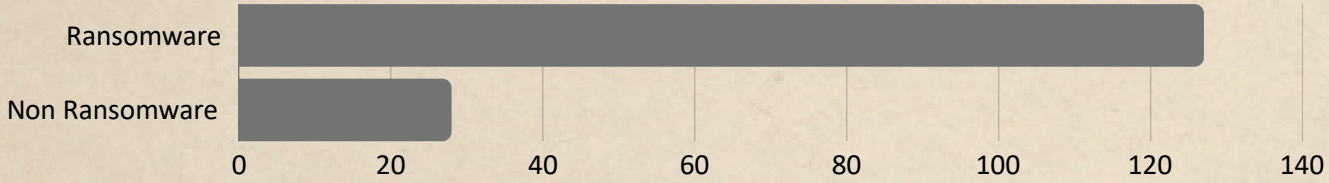
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:31MAY - 06 JUNE 2026

Affected Countries



Actor Distribution



Ransomware dominates the threat landscape with 127+ incidents, far outpacing 28 non-ransomware cases, making it the most prevalent and impactful attack type.

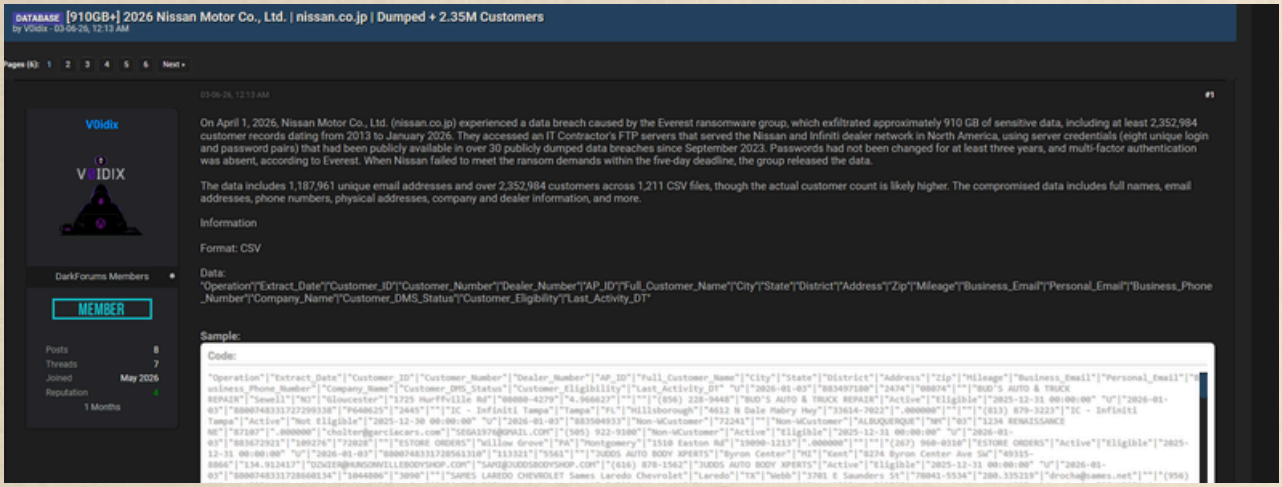
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 31 MAY - 06 JUNE 2026

Nissan Motor Co., Ltd Breach Incident

On June 03, 2026, a Japan company Nissan Motor Co., Ltd. suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: **Automotive Manufacturing and Financial Services**
Threat Actor : **Everest**
Data Sold: **910 GB**



Key Highlights

- **Data Exposure:** Approx. 2.35M customer records reportedly leaked, including names, emails, phone numbers, addresses, and dealer/customer data.
- **Threat Actor:** Linked to the Everest ransomware group
- **Threat Activity:** Data was allegedly posted on an underground forum with sample records provided.
- **Threat Level:** Critical, with risks of identity theft, phishing, social engineering, and fraud due to the large volume of exposed PII.

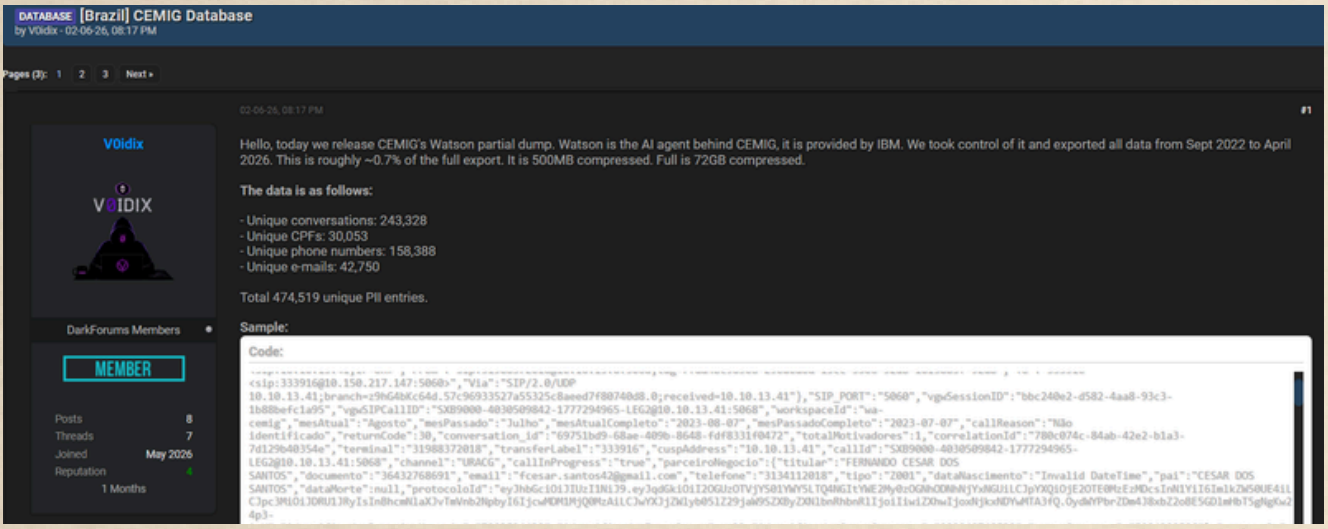
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 31 MAY - 06JUNE 2026

CEMIG Breach Incident

On June 02, 2026, a Brazil company CEMIG suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Utilities, Energy
Threat Actor : V0idix
Data Sold: 72GB



Key Highlights

- **Data Exposure:** Approx. 474K PII entries reportedly leaked from CEMIG's IBM Watson-based AI platform, including conversation records, CPF numbers, phone numbers, and email addresses.
- **Threat Actor:** Linked to V0idix
- **Threat Activity :** Data was allegedly published on an underground forum, with sample records provided and claims of access to a much larger dataset.
- **Threat Level:** High, with risks of identity theft, phishing, social engineering, and misuse of exposed customer information.

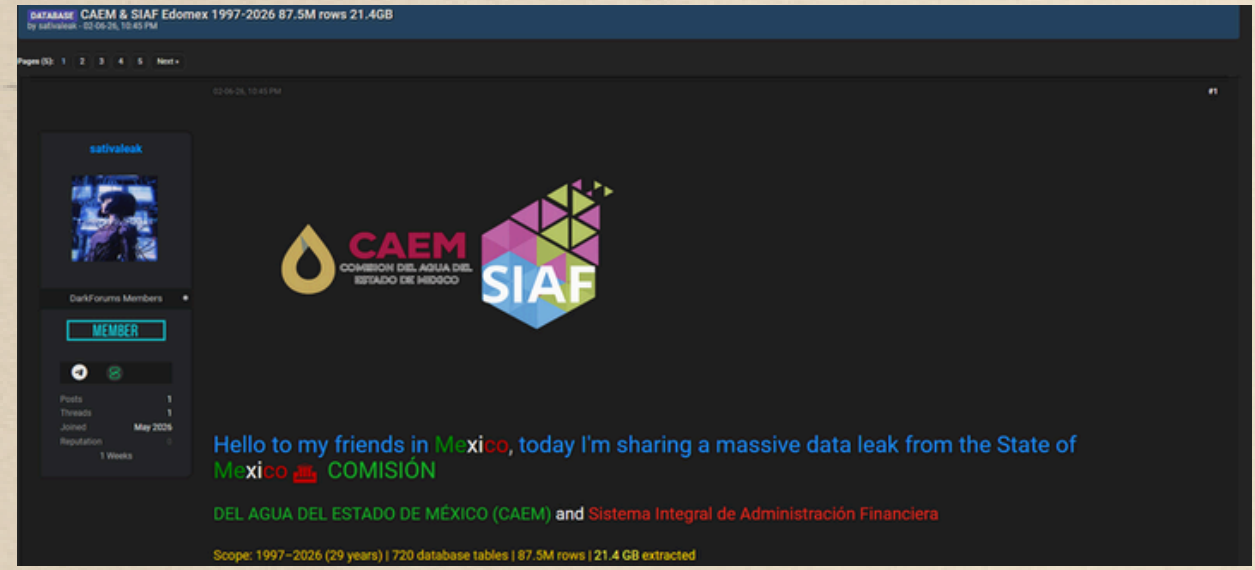
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:31 MAY - 06 JUNE 2026

CAEM Breach Incident

On June 02, 2026, a Mexico company CAEM suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: **Public Utilities (Water Management)**
Threat Actor : **sativaleak**
Data Sold: **21.4 GB**



Key Highlights

- **Data Exposure:** Approx. 87.5M records across 720 database tables reportedly leaked from CAEM and SIAF systems, spanning data collected between 1997–2026.
- **Threat Actor:** Linked to sativaleak.
- **Threat Activity:** Data was allegedly published on an underground forum, with claims of 21.4 GB of extracted information from government-related systems.
- **Threat Level:** Critical, due to the massive volume of records and potential exposure of sensitive administrative, financial, and citizen-related information, increasing risks of fraud, identity theft, and targeted attacks.

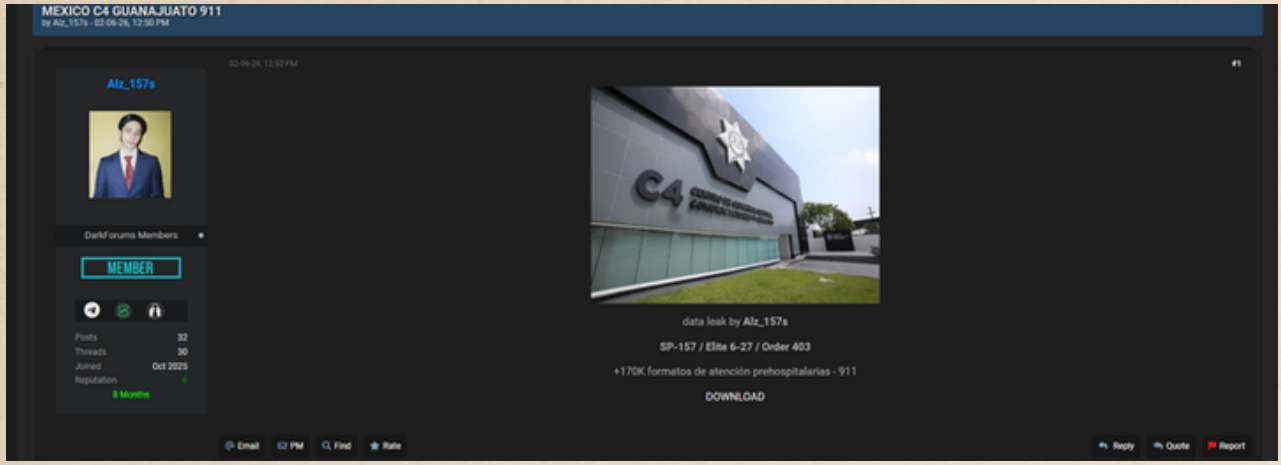
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:31 MAY - 06 JUNE 2026

C4 Guanajuato Breach Incident

On June 02, 2026, a Mexico company C4 Guanajuato suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector:Public Safety
Threat Actor : c0mmandor
Data Sold: 1.7 GB



Key Highlights

- **Data Exposure:** Approx. 170K+ pre-hospital emergency (911) records reportedly leaked from the C4 Guanajuato 911 system in Mexico.
- **Threat Activity:** Data was allegedly posted on an underground forum with downloadable files and references to emergency response records.
- **Threat Actor:** Linked to Alz_157s.
- **Threat Level:** High, as exposed emergency service records may contain sensitive personal and incident-related information, creating risks of privacy violations, identity theft, and targeted social engineering.

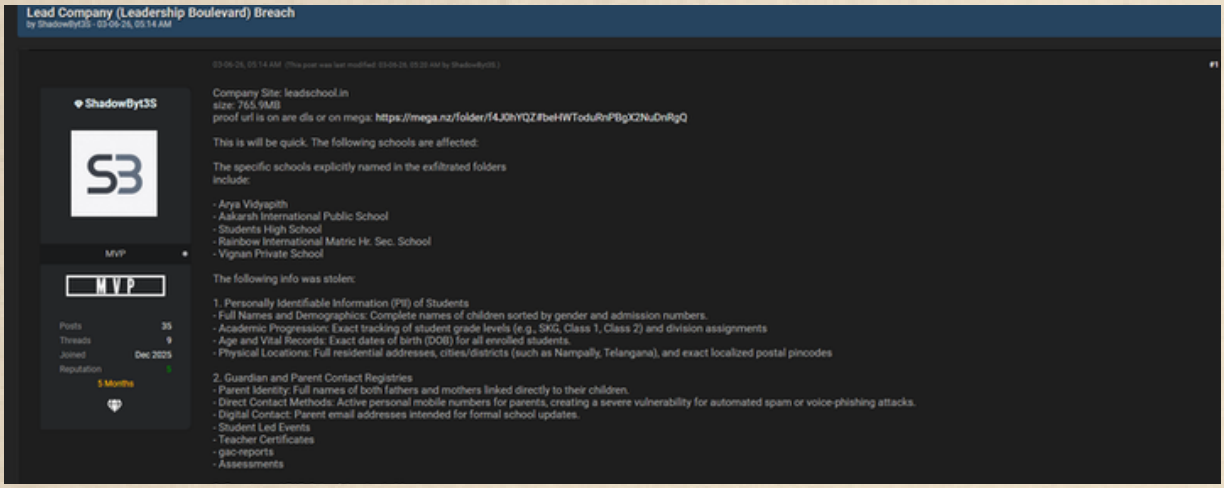
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:31 MAY - 06 JUNE 2026

LEAD Group Breach Incident

On June 03, 2026, a Indian company LEAD Group suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Education Technology
Threat Actor : ShadowByt3S
Data Sold: 765.9 MB



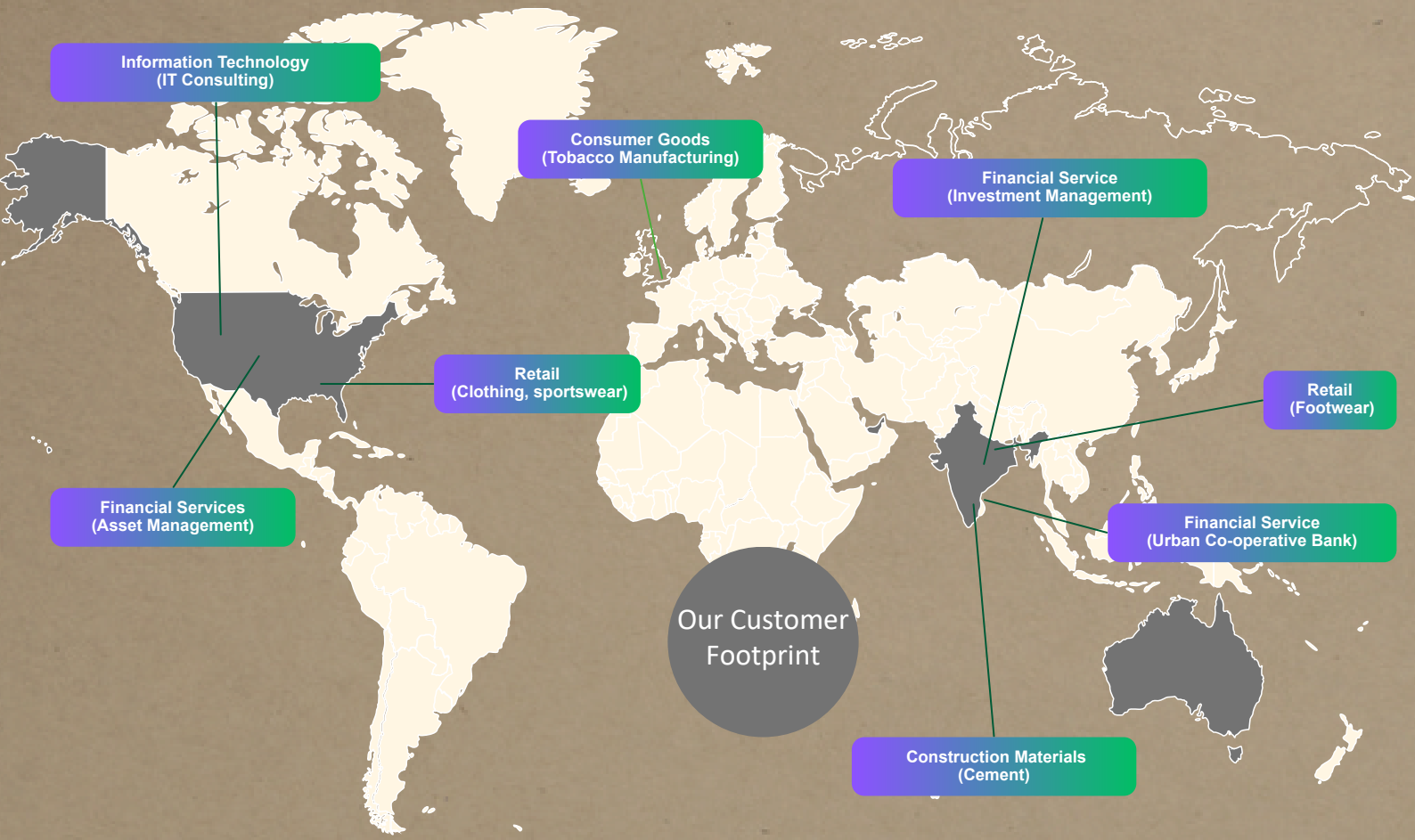
Key Highlights

- **Data Exposure:** Student, parent, and school records were reportedly leaked, including student names, demographics, dates of birth, addresses, academic details, parent names, phone numbers, and email addresses.
- **Threat Actor:** Linked to ShadowByt3S.
- **Threat Activity:** Data was allegedly posted on an underground forum with references to multiple affected schools and downloadable archives.
- **Threat Level:** High, due to the exposure of sensitive student and guardian information, creating risks of identity theft, phishing, social engineering, and privacy violations involving minors.

About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio

Secure Cloud WL

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

We create secure cloud environments, automate Cloud SecOps & manage it.

24x7 Monitoring

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

When it comes to SOC Monitoring & Response, we cover all aspects of it

Vuln Mgmt

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuin Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

Program designed VAPT Engagement to enhance protection & reduce attack surface

Threat Intel

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

We take threat intel maintenance, keep, usage & application to next level.

Data & Privacy

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

Data and privacy are two considerations, we design, implement it & run compliances

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995